<u>REMARKS/ARGUMENTS</u>

Favorable consideration of this application, as presently amended, is respectfully requested.

Claims 1, 3-5, 7-10, 12, 14, 15 and 17-25 are pending in the present application. Claims 7, 12, 14, 21 and 22 are amended by the present response. Support for amendments to the claims is found in the disclosure as originally filed, at least on page 41, lines 2+. Thus, no new matter is added.

In the outstanding Action, Claims 7-10, 12, 14, 21, 22 and 25 were rejected under 35 U.S.C. §103(a) as unpatentable over <u>Newcombe</u> (U.S. Pat. Pub. No. 2003/0172269) in view of <u>Arnold et al.</u> (WO 03/055170, herein "Arnold") and in further view of <u>Medvinsky</u> (U.S. Pat. Pub. No. 2003/0163693); and Claims 1, 3-6, 15, 17-20, 23 and 24 are allowed.

Initially, Applicants gratefully acknowledge the indication of the allowable subject matter in Claims 1, 3-6, 15, 17-20, 23 and 24.

Addressing now the rejection of Claims 7-10, 12, 14, 21, 22 and 25 under 35 U.S.C. §103(a) as unpatentable over <u>Newcombe, Arnold</u> and <u>Medvinsky</u>, Applicants respectfully traverse this rejection, at least, in light of the amendments to the independent claims.

Claim 7 recites, in part,

> a reception means for receiving an authentication request inclusive of a user authentication information and key information representing a public key K_{PU} of the user terminal both transmitted from the user terminal;
> an authentication means to which the user authentication information of the received authentication request is input and which authenticates the user on the basis of the user authentication information and providing a signal indicating a successful authentication upon a successful authentication;
> an address allocating means for allocating an address to the user terminal in response to an input of the signal indicating a successful authentication of the user;
> authentication information generating means for generating information-for-authentication using at least the allocated address and the key information;

> a ticket issuing means for issuing a ticket containing the allocated address, the key information, and the information-for-authentication to the user terminal, <u>the application server conducting authentication for providing services to the user terminal based on the ticket, the ticket guaranteeing a correspondence between the user authenticated by the authentication means, the allocated address, and the key information corresponding to the user terminal</u>; and
> a ticket transmitting means to which the ticket is input and which transmits the ticket to the user terminal.

Independent Claims 12, 14, 21 and 22 recite similar features with regard to the ticket guaranteeing a correspondence between the user authenticated by the authentication means, the allocated address, and the key information corresponding to the user terminal.

Newcombe describes an authentication server that incorporates local and remote IP addresses received from a client into a ticket and provides the ticket to the client. Furthermore, in Newcombe, the content server compares the IP address in the ticket with the IP address of a packet (source address of the packet) from a client[1] and, if they match, authentication of the client is performed[2] and the content ticket is verified[3] with a content then being sent to the client.[4]

Arnold describes a system in which a network access server 118 allocates a first IP address to an authenticated user and a server instance (middleware) 110 allocates a second IP address to the user who has accessed the server instance 110 using the first IP address. The server instance 110 serves as a middleware for the user to access e-service providers 100, 102. The server instance 110 neither issues tickets nor receives any information corresponding to the key information.

---

[1] See Newcombe, Fig. 12, step 1210.
[2] See Newcombe, Fig. 13, step 1304.
[3] See Newcombe, Fig. 13, step 1306.
[4] See Newcombe, Fig. 13, step 1308.

Medvinsky describes that a public key of a client is sent to KDC (Key Distribution Center which acts as an authentication server). In Medvinsky public keys are sent to conduct key-sharing through cryptographic computation between a client and a server.

The outstanding Action asserts on pages 3-9 that Claims 7 and 12 are obvious in view of Newcombe, Arnold and Medvinsky, Applicants respectfully traverse this assertion.

Specifically, regarding Claim 7, the outstanding Action states beginning on page 4, 5th line from the bottom to page 5, line 1, that Newcombe teaches "authentication information generating means for generating information-for-authentication using at least the allocated address and the key information (paragraph [0025] and [0029])" and "a ticket issuing means for issuing a ticket containing the allocated address, the key information, and the information-for-authentication" [0025].

Applicants note that paragraph [0025] of Newcombe describes various operations and information dealt by the client (user terminal). However, in paragraph [0025] of Newcombe, there is no description about anything similar to the key information recited in the claimed invention.

According to the claimed invention, the key information represents a public key K_{PU} of the user terminal. In a non-limiting example, page 28, lines 23-27 of the present specification illustrates that the key information may include the public key itself, a certificate including the public key or hashed value of the public key. In the claimed invention, the public key is utilized between the user terminal and an *application server* so that the application server can verify that the packets received from the user terminal are not forged. The authentication server receives the key information together with the user authentication information from the user terminal, and the authentication information generating means of the authentication server generates information-for-authentication using

21

the key information and the allocated address. The ticket issuing means generates a ticket

containing the information-for-authentication, the key information and the allocated address.

It should be noted that according to Newcombe, the session key (not such an

asymmetric key as public key but a symmetric key[5]) contained in both a client readable

portion and a server readable portion of a ticket is intended to be used for establishing a

session through cryptographic protocol.[6] In contrast, in the claimed invention, the

authentication information generating means of the authentication server does not use the key

information for cryptographic purpose. Rather, the key information is used as data (a bit

sequence) for generating the information-for-authentication. Moreover, the information-for-

authentication is included in the ticket together with the allocated address and the key

information so that the authentication server can guarantee to the application server that the

1) authenticated user, 2) the allocated address, and 3) the key information (e.g. the related

public key) are associated with each other as was explained on page 6, lines 12-18 of the

Supplemental Remarks filed December 29, 2009.

In other words, in the authentication server of the claimed invention, the public key is

used to guarantee the relationships between the user terminal corresponding to the public key

and the address allocated to the user terminal, without the need to perform any cryptographic

computation using the key information. The application server uses the relationships to

conduct address based authentication for communication with the user terminal.[7]

Thus, the modified authenticator described in paragraph [0025] of Newcombe is a

combination of a timestamp and client's local and remote IP addresses, and does not include a

public key and, therefore, differs from the key information recited in the claimed invention.

Furthermore, the local and remote IP addresses associated with the client also do not have

---

[5] See paragraph [0032] of Newcombe
[6] See paragraph [0065] of Newcombe
[7] Based on description at page 41, lines 2-4.

any relationship with the key information. In paragraph [0029] of Newcombe, the well-known typical asymmetric cryptosystems such as the RSA scheme and its variations (OAEP with SHA1) are described as examples of a scheme of encrypting a ticket. However, such a configuration does not have anything to do with the key information recited in the claimed invention. This is the case, at least, because the authentication server recited in the claimed invention does not use the key information as an encryption key for cryptographic computation. Therefore, it is apparent that the paragraphs [0025] and [0029] of Newcombe contain neither any description similar to the key information nor any description corresponding to the authentication information generating means for calculating the information-for-authentication using at least the key information (and the allocated address) as recited in Claim 7.

The outstanding Action asserts in the bottom five lines on page 5 that "Medvinsky teaches a ticket granting protocol in which the client and server perform a Diffie-Hellman exchange that includes each side sending their respective public key to the other side (0030, 0031)" and further that "Thus, the client sends its public key to the server.' However, Applicants note that the claimed invention differs from Medvinsky in how a public key (or key information) is utilized. In Medvinsky, public keys are sent to conduct key-sharing through cryptographic computation between a client and a server. Applicants note that this is the typical method and reason to send a public key to a counterpart when a client implements a public key protocol with a counterpart to establish a session.

In contrast, in the claimed invention, the key information is sent to the authentication server not to implement cryptographic protocol between the user terminal and the authentication server but to be used by the authentication server to generate the information-for-authentication that guarantees the correspondence between the authenticated user, the allocated address and the key information as noted above.

In other words, the key information recited in the claimed invention is used as binary data or a bit string by the authentication information generating means of the authentication server to calculate information-for-authentication. Thus in a non-limiting example explained at page 28, lines 23-27 of the present specification, the key information does not need to be a public key itself, but may be a hashed value of the public key. On the contrary thereto, in Medvinsky, it is necessary to perform key-sharing using a public key based on the Diffie-Hellman algorithm[8] and, therefore, if a hashed value of the public key is sent instead of the public key, cryptographic computation cannot be performed correctly, resulting in a failed key-sharing.

With regard to Claim 12, the outstanding Action asserts that Newcombe teaches ".... a ticket reception means for receiving a ticket transmitted from the authentication server (0064), key information (0029), and information-for-authentication produced by using at least the allocated address and the key information (0065)," and "a key information generating means to which a public key of the user terminal is input (0025 and 0029)."

However, Applicants respectfully submit that Newcombe does not describe anything similar to the key information as explained above in connection to Claim 7. Moreover, the Examiner's assertion does not match the Examiners statement at page 9, lines 9-19 that "Newcombe is silent in explicitly teaching the key information represents the public key of the client and that is sent along with the user authentication information."

It is emphasized that the effect of enclosing the information-for-authentication, the key information and the allocated address into a ticket is to guarantee to the application server that the allocated address and the key information (and therefore the user terminal) are associated with each other. In Claim 12, the public key of the user terminal enables: first, that the relationship between the allocated address and the user terminal is guaranteed; and

---

[8] See paragraph [0049] of Medvinsky

second, a session secret key to be generated by the application server. Medvinsky describes

nothing about guaranteeing a relationship between the allocated address and the user terminal

is guaranteed.

Thus, Applicants respectfully submit that Claim 12 is not obvious based on the

disclosure from the combination of Newcombe, Arnold and Medvinsky.

Moreover, regarding Claim 14, the outstanding Action states that "Newcombe teaches

a user terminal .... comprising: a ticket reception means for receiving .... information-for-

authentication produced .... ; a key information generating means .... which generates a key

information by processing random number by the authentication purpose shared secret key

(0031); .... a user authentication information transmitting means configured to transmit the

key information together with the user authentication information to the authentication server

(0052 and 0072)." Applicants respectfully traverse this assertion at least for the reasons

noted above with regard to Claim 12. Applicants note that a difference between Claims 12

and 14 resides in that instead of using the public key of the user terminal, Claim 14 generates

the key information using a shared secret key which is shared with the application server.

However, the application of the key information is the same as in Claim 12. Therefore,

Claim 14 also is not obvious from the disclosure of the combination of Newcombe, Arnold

and Medvinsky.

Accordingly, Applicants respectfully submit that Claims 7, 12, 14, 21 and 22 and

claims depending respectfully therefrom, patentably distinguish over Newcombe, Arnold and

Medvinsky considered individually or in combination.

Consequently, in view of the present amendment, no further issues are believed to be

outstanding in the present application, and the present application is believed to be in

condition for formal allowance. A Notice of Allowance for the claims is earnestly solicited.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, L.L.P.

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 07/09)
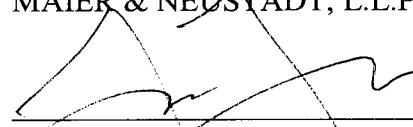
James J. Kulbaski
Attorney of Record
Registration No. 34,648
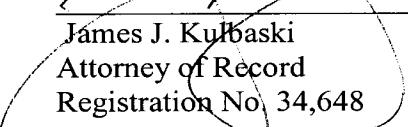
James Love
Registration No. 58,421

3666190_1

26